

LISTING OF CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment, comprising the steps of:
 - a. creating a public-private key pair within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message;
 - b. storing the private key within the device against the possibility of divulgement thereof by the device; and
 - c. securely linking the public key with other information by storing the public key in ~~association with~~ and the other information in a database within the secure environment.
2. (Original) The method of claim 1, wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device.
3. (Original) The method of claim 2, wherein each digital signature generated by each device is a random number.
4. (Previously Presented) The method of claim 1, wherein the other information comprises respective security features and a manufacturing history of each device.
5. (Previously Presented) The method of claim 1, further comprising the step of identifying a particular manufactured device by authenticating a message using one of a plurality of public keys in the database within the secure environment, a digital

signature for the message having been generated by the particular manufactured device.

6. — 20. (Cancelled)

21. (Previously Presented) The method of claim 1, wherein the public key and information linked therewith is obtained from a Secure Entity.

22. (Currently Amended) The method of claim 1, wherein the ~~PuK-linked~~ other information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

23. (Currently Amended) The method of claim 22, wherein the ~~PuK-linked-account~~ public key and the other information ~~of the users~~ is indexed in the database by unique account identifiers such that the ~~PuK-linked-account~~ public key and the other information for a user is retrievable from the database based on the account identifier.

24. (Currently Amended) The method of claim ~~22~~ 23, wherein the public key is the unique account identifier.

25. (Currently Amended) The method of claim 1, wherein the ~~PuK-linked~~ public key and the other information ~~maintained~~ stored in the database for each user further includes user-specific information.

26. (Currently Amended) The method of claim ~~12~~ 25, wherein the user-specific information includes the name and address of the user.

27. (Currently Amended) The method of claim ~~6~~ 1, further comprising the step of establishing an account on behalf of a user of a device with a third-party by

communicating the public key of the device and the other information linked with the public key from the database to the third-party.

28. (Currently Amended) The method of claim 27 1, wherein the public key of the device and the other information linked with the public key is communicated to a third party upon the request of the third-party.
29. (Currently Amended) The method of claim 1 further comprising the step of updating the ~~PK-linked accounts~~ public key of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:
- a. receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefor,
 - b. authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof,
 - c. sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.
30. (Previously Presented) The method of claim 29, further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier.
31. (Previously Presented) The method of claim 29, further comprising the step of sending the EC received from the user to each of the third-parties.

REMARKS

Claims 1–5 and 21–31 are pending in this application. In a final rejection mailed February 21, 2006, the examiner made the following rejections: